Transnational Threats:
Blending Law Enforcement and Military Strategies

Compiled by

Rye Barcott
University of North Carolina
Chapel Hill

The United States Army War College, the Triangle Institute for Security Studies, and the Duke University Center for Law, Ethics, and National Security co-sponsored a conference in Chapel Hill, North Carolina, from February 2-3, 2000, to explore how military and law enforcement strategies could be integrated better to counter transnational threats. The conference was well attended by approximately 90 key people from across the Department of Defense (DoD), the Federal Bureau of Investigation, the National Security Council, business, the drug control community, academia, and the congressional staff. As one might expect, the discussion generated by this eclectic group was intense, thought provoking, and informative. The discussants focused on three key and interrelated transnational threats: terrorism involving weapons of mass destruction (WMD), cyber threats to the national infrastructure, and international organized crime. This brief summary highlights some of the salient points raised during the conference. The U.S. Army War College Strategic Studies Institute plans to publish a comprehensive conference report later this year.

Terrorism *was defined broadly as the use of psychological warfare to achieve political goals.* Contemporary terrorist networks typically are not state-sponsored. Their aims and objectives are less easily defined than those of traditional terrorist groups. Although the accessibility of nuclear, biological, and chemical WMD has increased, the probability of terrorists using WMD effectively in the future remains low, in part because of high acquisition, testing, and managerial costs, and in part because terrorists can achieve their goals without causing the use of WMD. Thus, the threat of terrorism involving WMD is less than generally assumed. Nevertheless, rapid technological innovation and opposition to perceived U.S. hegemony suggest that future terrorist use of WMD cannot be precluded. Furthermore, a review of terrorist incidents over the past decade reveals a trend toward fewer but more destructive attacks.

Cyber threats *were defined as information warfare attacks on the U.S. information infrastructure in order to disrupt or undermine the government, and cyber-crime, which refers to attacks on information systems for personal or organizational gain.* These threats are serious, especially if executed in conjunction with more conventional military hostilities directed against the United States. The national economy as well as DoD systems are vulnerable to cyber attacks. Furthermore, cyber crimes are increasing, and orchestrated information warfare against the United States can be expected in the future. Terrorist organizations will be the most common perpetrators of information warfare, but state-on-state information warfare also is a distinct possibility. To date, rapid technological innovations coupled with lagging legal authorities have positioned the U.S. Government in a continual "catch-up" situation where it mounts largely ineffective responses to, so far, limited number of "hi-tech" threats.

Organized crime *was defined as the continuation of business by criminal means.* Criminal organizations have increased in size, scope, and power. They are more decentralized, cross-cultural, and international than in the past. The threats posed by organized crime to the United

States are less immediate than they are to other nations, but are still serious. Organized crime can threaten the stability of strategically important states by instigating corruption and eroding, if not supplanting, legitimate governments. Moreover, an increase in organized crime corresponds to an increase in global drug trafficking and money laundering--two conditions which directly and indirectly threaten U.S. national security.

Strategic Challenges .

In the past, the roles of the military and law enforcement agencies were relatively distinct: the military dealt principally with threats from beyond U.S. borders, while police forces dealt mostly with internally generated threats. Such is not the case today for at least two reasons. First, crime has taken on international dimensions. Second, it is more difficult today to identify the nature and source of transnational threats. The distinction between what is a crime and what is an attack warranting a military response is often unclear. But, given the current state of U.S. interagency organization, this distinction is crucial in order to determine which governmental agency should have the lead responsibility for countering a threat to U.S. security.

Transnational threats present significant problems for law enforcement. Domestic law is often incompatible with international law and, without foreign cooperation, the United States has no authority to exercise jurisdiction within the territory of foreign sovereigns. "Venue" is tied to sovereignty, yet transnational perpetrators of attacks and crimes often operate outside the domain of and across sovereign borders. Frequently, information needs to be shared among U.S. Government agencies and with the agencies of other governments in order to prosecute cases involving transnational threats. However, U.S. federal agencies, much less those of other states, are not optimally organized to facilitate effective communication and information sharing.

Transnational threats often directly or indirectly affect the U.S. information infrastructure, which is primarily controlled by the private sector. It is in the interest of U.S. national security for government agencies to work with the private sector to gain legitimate access to essential electronic hardware and software. The private sector, however, is extremely reluctant to enter into a public-private partnership for two reasons. First, it fears increased government regulation. Information truly is power in today's economy. Members of the private sector want to vie for information power advantages without the constraints of cumbersome governmental regulation. Second, and more importantly, government meddling through regulation can lead to publication of commercial enterprise vulnerability to information attacks. What can easily result is catastrophic business losses as customer and investor confidence in the victimized enterprise plummets. Furthermore, effective government regulation is made more challenging by the drain of information expertise from the public sector brought on by highly competitive salaries offered by the private sector.

Strategies for Improvement .

Just as criminal organizations are forming flexible, reactive networks, the federal government needs to break interagency barriers and pursue fundamental restructuring of the national capability to prevent and, when necessary, respond to transnational threats. This will require a governmental refocus on prediction, preemption, and quick responses to transnational threats, particularly cyber threats, and a push towards "jointness" among the civilian agencies of government. Working together, the Executive Branch, through the planning and budgeting processes, and Congress, through the appropriations and authorizations processes, can effect real

change. However, first there must be changes in the processes themselves. In particular, the DoD program, planning, and budget process is outdated and needs to be restructured. Congress should request a new, information age process from the Executive Branch, hold hearings, review laws, and make necessary revisions to the manner in which the DoD formulates strategy and determines the means required for implementation. But the Executive Branch and Congress must move beyond the reformation of DoD processes and craft a more effective interagency process. Responsible officials need to consider "out of the box thinking," such as agency mergers or the identification of a "czar" with adequate supra-agency authority.

Furthermore, coordination and cooperation within the federal government must extend to state and local governments and the private sector "information industry." Cooperation between the federal government and the private sector will benefit both government and business. The U.S. Government should consider using its position as a major buyer in the market to demand industry standards on security measures. Woefully, intelligence gathering is still based largely on a Cold War model and must be changed. A possible first step focuses on the gap between intelligence gathering and law enforcement. Federal laws, including the Fourth Amendment of the U.S. Constitution, restrict the use of national intelligence for domestic law enforcement. New laws need to be developed to bridge the gap between the traditional use of intelligence to prosecute criminal cases, and strategic intelligence which is used to predict, preempt, and defend against attacks on the United States and its citizens.

New educational initiatives should be undertaken to ensure U.S. sustained technological superiority and to increase public understanding of transnational threats. Education initiatives will foster more measured and rational policy responses to transnational threats. Finally, most conference participants seemed to agree that transnational threats are increasingly nonmilitary in nature and call for nonmilitary solutions. Nonetheless, secondary and tertiary functions of the U.S. armed forces are of increasing importance to law enforcement, especially the military's ability to provide transportation, emergency medical care, translators, and large-scale disaster relief and humanitarian assistance.

* * * * *

* * * * *